EPITECH.
PARIS GRADUATE SCHOOL OF DIGITAL INNOVATION

Security

Kickoff

T7 - MSc Pool

T-POO-700

What is computer security?

- protect the integrity of information technologies (systems, networks, computer data) against attacks, damage or unauthorized access

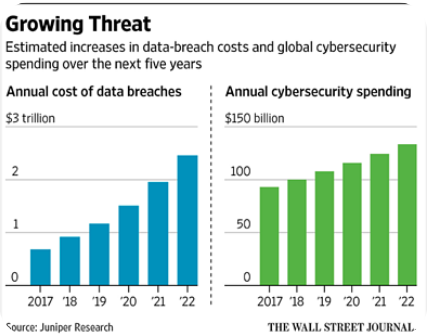
What is computer security?

- protect the integrity of information technologies (systems, networks, computer data) against attacks, damage or unauthorized access
- based on a regular system feedback usually managed through automated checkpoints

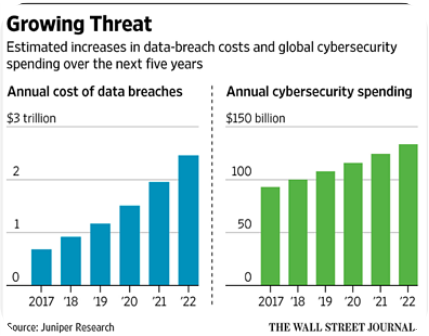
What is computer security?

- protect the integrity of information technologies (systems, networks, computer data) against attacks, damage or unauthorized access
- based on a regular system feedback usually managed through automated checkpoints
- needs to be integrated right from the design stage

Figures from 2019

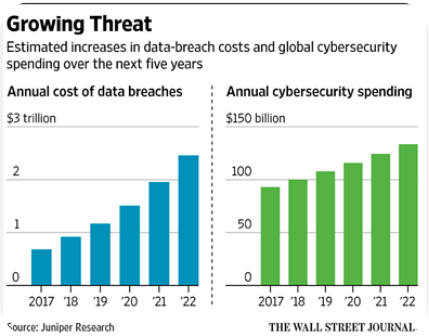


Figures from 2019



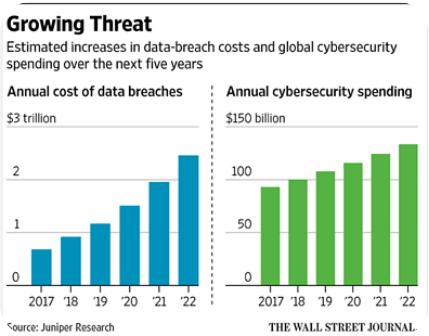
- 1.1 million bank card fraud victims per year

Figures from 2019



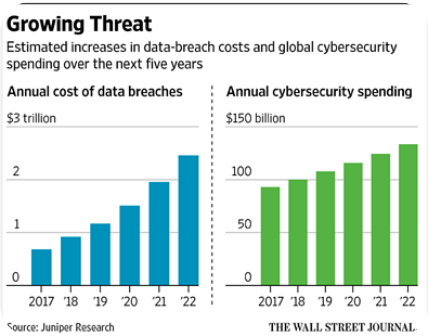
- 1.1 million bank card fraud victims per year
- 65 data leaks per second

Figures from 2019



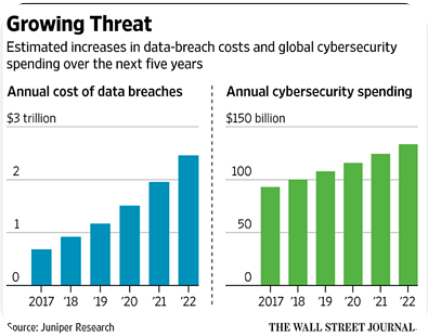
- 1.1 million bank card fraud victims per year
- 65 data leaks per second
- 140 phishing attacks per hour

Figures from 2019



- 1.1 million bank card fraud victims per year
- 65 data leaks per second
- 140 phishing attacks per hour
- average companies suffer 29 cyberattacks a year

Figures from 2019



- 1.1 million bank card fraud victims per year
- 65 data leaks per second
- 140 phishing attacks per hour
- average companies suffer 29 cyberattacks a year
- 96% of websites have vulnerabilities

Old-fashioned VS new way

- Traditionally, IT security was about strengthening, maintaining and patching. Experts reviewed codes and systems to secure them.

Old-fashioned VS new way

- Traditionally, IT security was about strengthening, maintaining and patching. Experts reviewed codes and systems to secure them.

- But attackers are getting fast and plentiful, some attacks are automated and weaknesses can become very costly.

Old-fashioned VS new way

- Traditionally, IT security was about strengthening, maintaining and patching. Experts reviewed codes and systems to secure them.
- But attackers are getting fast and plentiful, some attacks are automated and weaknesses can become very costly.
- Now security programs are adapted to be continuous, integrated, flexible. It is a shared concern amongst all the IT actors.

Vulnerability

weakness of a system

It could be:

Vulnerability

weakness of a system

It could be:

- design flaw

Vulnerability

weakness of a system

It could be:

- design flaw
- implementation bug

Vulnerability

weakness of a system

It could be:

- design flaw
- implementation bug
- unchecked user input

Vulnerability

weakness of a system

It could be:

- design flaw
- implementation bug
- unchecked user input
- irrelevant access restriction

Vulnerability

weakness of a system

It could be:

- design flaw
- implementation bug
- unchecked user input
- irrelevant access restriction
- ….

Vulnerability

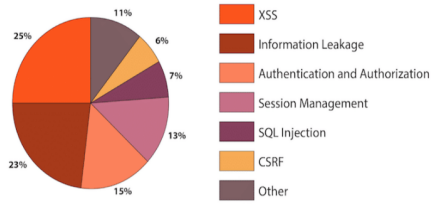
weakness of a system

It could be:

- design flaw
- implementation bug
- unchecked user input
- irrelevant access restriction
- ….

There is an unlimited number of vulnerabilities, but some organizations have conducted studies to identify the most common.

Most common vulnerabilities in 2017



OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

Pentesting

PENetration **TEST**ing

Pentesting

PENetration **TEST**ing

- use of penetration tools (some predetermined, some that you design yourself) to simulate cyberattacks in real life

Pentesting

PENetration **TEST**ing

- use of penetration tools (some predetermined, some that you design yourself) to simulate cyberattacks in real life
- ethical hacking (vs real hackers)

Pentesting

PENetration **TEST**ing

- use of penetration tools (some predetermined, some that you design yourself) to simulate cyberattacks in real life
- ethical hacking (vs real hackers)
- you only have a few days to compromise the systems

Pentesting

PENetration **TEST**ing

- use of penetration tools (some predetermined, some that you design yourself) to simulate cyberattacks in real life
- ethical hacking (vs real hackers)
- you only have a few days to compromise the systems
- document and explain your methods and results

Methodology

5. Exfiltrate & Protect

Discovered credentials and data are exfiltrated while covering tracks and remaining undetected.
This directly tests your organizations ability to detect and mitigate sensitive information as it leaves your network before its sold on the black market.

1. Attack Scope

Targets are defined and prioritized within the scope of the organization. Important hosts are noted, but, NWG focuses on the infrastructure as a whole.

4. Gain Foothold

Outbound connection is initiated and access is expanded to obtain credentials and strengthen hold. This gives you insight on an attackers ability to maintain long term access to your network.

2. OSINT & Tools

Open Source Intelligence is leveraged to research the origanization like a real attacker would. Tools are built and acquired to respond to the infrastructure appropriately.

3. Intrusion

Testing for detection followed by deploying methods to reach initial intrusion. This will directly test your organizations ability to detect and mitigate real threats from the perimeter to the host.

Any questions

?